FIG. 1

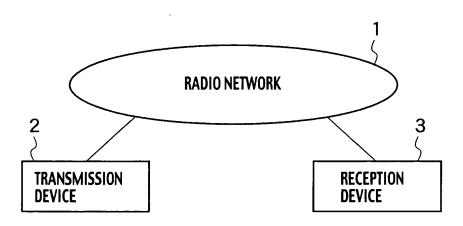
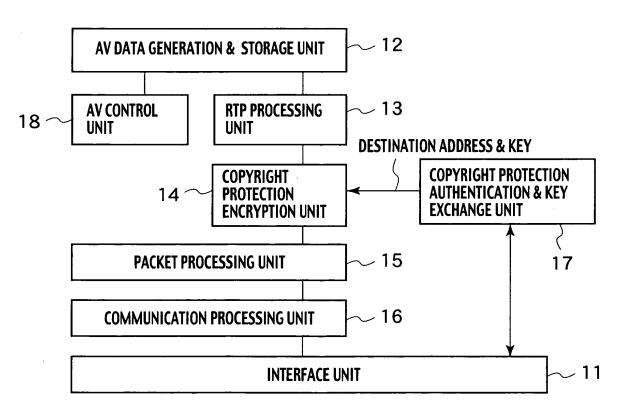


FIG. 2



2/14



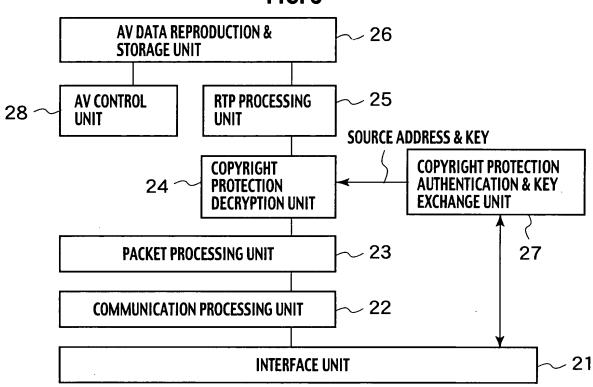
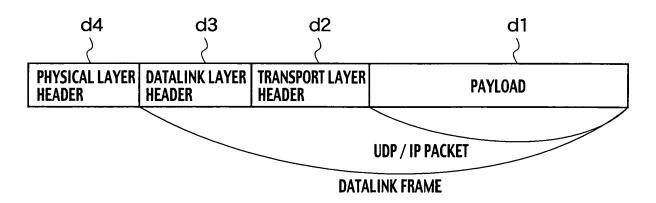


FIG. 4



### FIG. 5

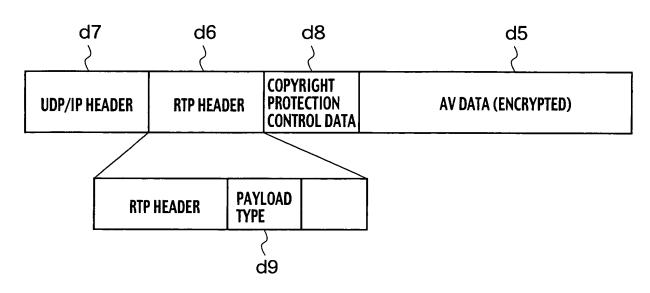
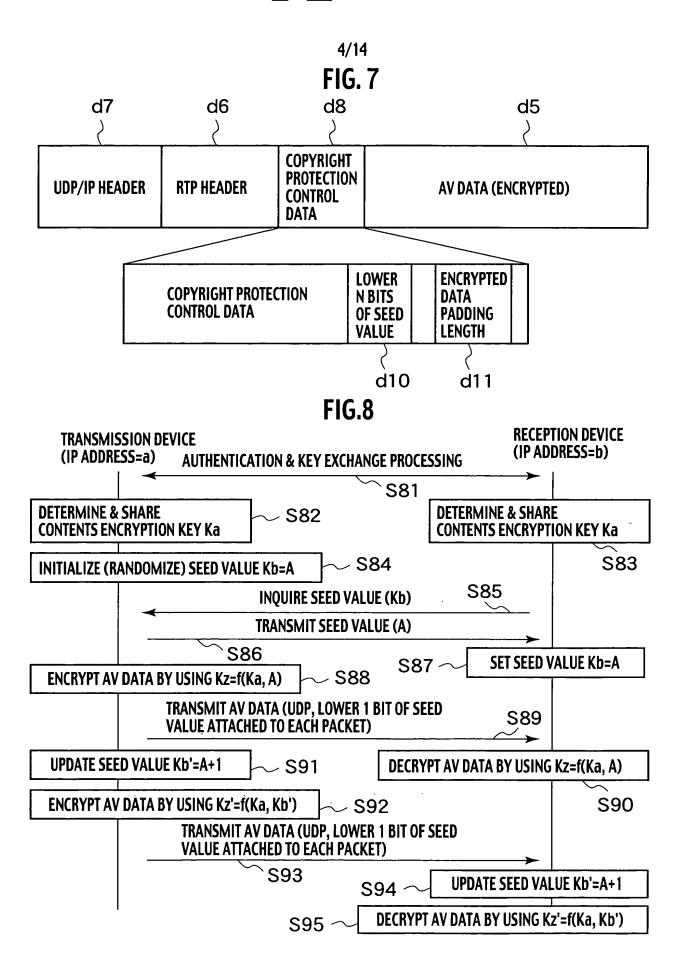
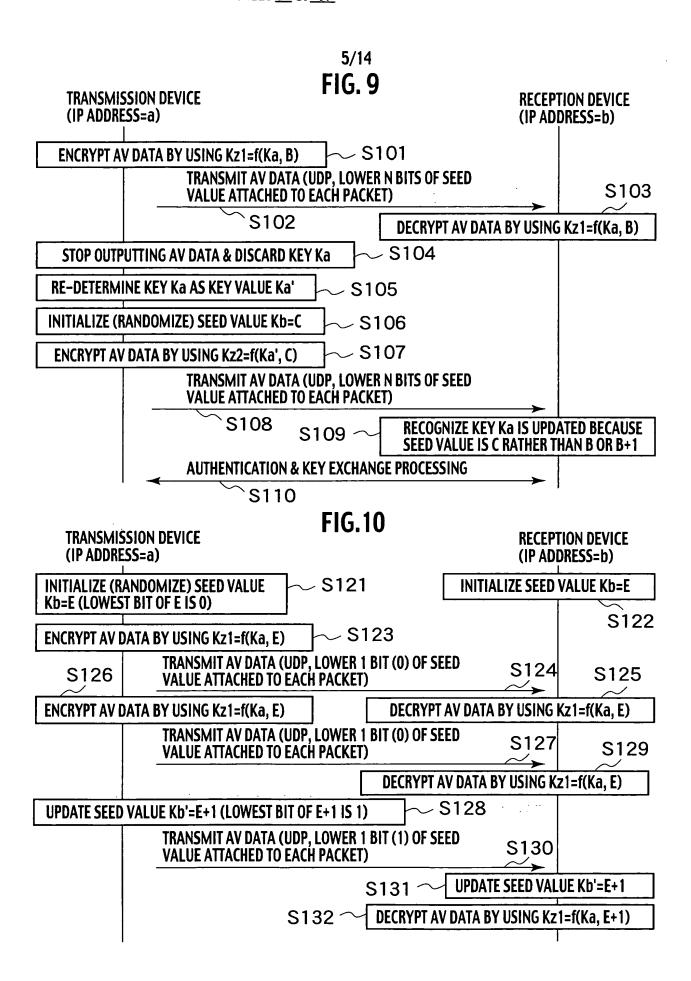


FIG.6

TRANSMISSION DEVICE **RECEPTION DEVICE** (IP ADDRESS=a) (IP ADDRESS=b) AV CONTROL COMMAND (PLAY) (BY RTSP/TCP/IP), PT NEGOTIATION (PT=#z) S1 **ENCRYPT AV DATA** - S2 AV DATA (ENCRYPTED) (BY RTP/IP) **S3** (TRANSMISSION PORT #=#x, RECEPTION PORT #=#y, PT=#z) **AUTHENTICATION & KEY EXCHANGE REQUEST** (BY IP PACKET OR ETHERNET FRAME) FOR STREAM OF (TRANSMISSION IP ADDRESS=a, PORT #=#x, RECEPTION IP ADDRESS=b, PORT #=#y, TP=RTP, PT=#z) **AUTHENTICATION & KEY EXCHANGE PROCEDURE** (BY IP PACKET, OR PHYSICAL LAYER OR DATALINK LAYER FRAME) **S5 ACQUIRE DECRYPTION KEY** S6<sup>-</sup>



OBLON, SPIVAK, ET AL DOCKET #: 249170US2RD INV: Takeshi SAITO, et al. SHEET 5 OF 14



6/14 FIG. 11 TRANSMISSION DEVICE RECEPTION DEVICE (IP ADDRESS=a) (IP ADDRESS=b) **ENCRYPT AV DATA BY USING Kz1=f(Ka, E)** - S141 TRANSMIT AV DATA (UDP, LOWER 1 BIT (0) OF S143 SEED VALUE ATTACHED TO EACH PACKET) S144 S142 DECRYPT AV DATA BY USING Kz1=f(Ka, E) UPDATE SEED VALUE Kb'=E+1 (LOWEST BIT OF E+1 IS 1) LOST ON COMMUNICATION TRANSMIT AV DATA (UDP. LOWER 1 BIT (1) OF PATH SEED VALUE ATTACHED TO EACH PACKET) LOST ON S145 COMMUNICATION TRANSMIT AV DATA (UDP, LOWER 1 BIT (1) OF PATH SEED VALUE ATTACHED TO EACH PACKET) S146 **UPDATE SEED VALUE Kb"=E+2 (LOWEST BIT OF E+2 IS 0)** TRANSMIT AV DATA (UDP. LOWER 1 BIT (0) OF S148 S147 SEED VALUE ATTACHED TO EACH PACKET) DECRYPT AV DATA BY USING Kz1=f(Ka, E) S149 -**DECRYPTION FAILS** S150 -**FIG. 12** TRANSMISSION DEVICE RECEPTION DEVICE (IP ADDRESS=a) (IP ADDRESS=b) **ENCRYPT AV DATA BY USING Kz1=f(Ka, E)** - S161 TRANSMIT AV DATA (UDP. LOWER BITS (000) OF S162 S164 S163 SEED VALUE ATTACHED TO EACH PACKET) DECRYPT AV DATA BY USING Kz1=f(Ka, E) UPDATE SEED VALUE Kb'=E+1 (LOWER BITS OF E+1 IS 001) LOST ON **COMMUNICATION** TRANSMIT AV DATA (UDP, LOWER BITS (001) OF PATH SEED VALUE ATTACHED TO EACH PACKET) LOST ON S165 COMMUNICATION TRANSMIT AV DATA (UDP, LOWER BITS (001) OF PATH SEED VALUE ATTACHED TO EACH PACKET) **S166 UPDATE SEED VALUE Kb"=E+2 (LOWER BITS OF E+2 IS 002)** TRANSMIT AV DATA (UDP. LOWER BITS (002) OF S168 S167 SEED VALUE ATTACHED TO EACH PACKET) S169 ~ **UPDATE SEED VALUE Kb"=E+2** DECRYPT AV DATA BY USING Kz1=f(Ka, E+2) S170 -**DECRYPTION SUCCEEDS** S171 -

### **FIG. 13**

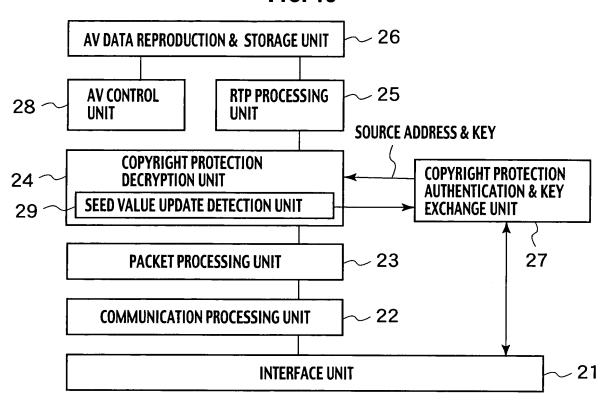


FIG. 14

TRANSMISSION DEVICE (IP ADDRESS=a)

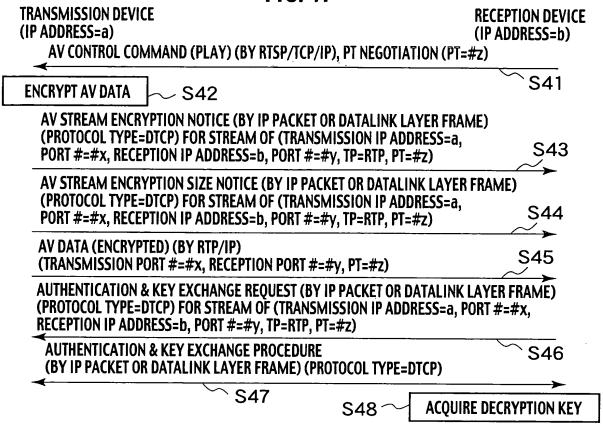
RECEPTION DEVICE (IP ADDRESS=b)

AV CONTROL COMMAND (PLAY) (BY RTSP/TCP/IP), PT NEGOTIATION (PT=#z) **S11 ENCRYPT AV DATA** - S12 AV DATA (ENCRYPTED) (BY RTP/IP) **S13** (TRANSMISSION PORT #=#x, RECEPTION PORT #=#y, PT=#z) AV STREAM ENCRYPTION NOTICE (BY IP PACKET OR DATALINK LAYER FRAME) (PROTOCOL TYPE=DTCP) FOR STREAM OF (TRANSMISSION IP ADDRESS=a. **S14** PORT #=#x, RECEPTION IP ADDRESS=b, PORT #=#y, TP=RTP, PT=#z) AUTHENTICATION & KEY EXCHANGE REQUEST (BY IP PACKET OR DATALINK LAYER FRAME) (PROTOCOL TYPE=DTCP) FOR STREAM OF (TRANSMISSION IP ADDRESS=a, PORT #=#x, RECEPTION IP ADDRESS=b, PORT #=#y, TP=RTP, PT=#z) **AUTHENTICATION & KEY EXCHANGE PROCEDURE S15** (BY IP PACKET OR DATALINK LAYER FRAME) (PROTOCOL TYPE=DTCP) <sup>−</sup> S16 **ACQUIRE DECRYPTION KEY** S17

## FIG. 15

FIG. 15						
TRANSMISSION DEVICE (IP ADDRESS=a)	RECEPTION DEVICE (IP ADDRESS=b)					
AV CONTROL COMMAND (PLAY) (BY RTSP/TCP/IP), PT NEGOTIATION (PT=	•					
AV DATA DESIGNATION (BY HTTP)	S21					
DESIGNATED CONTENTS IS DATA FOR WHICH COPYRIGHT PROTECTION IS REQUIRED \$23	∽\$22					
ENCRYPT AV DATA S24						
AV DATA (ENCRYPTED) (BY RTP/IP) (TRANSMISSION PORT #=#x, RECEPTION PORT #=#y, PT=#z)	S25					
AV STREAM ENCRYPTION NOTICE (BY HTTP RESPONSE OR SDP) (PROTOCOL TYPE=DTCP) FOR STREAM OF (TRANSMISSION IP ADDRESS=a, PORT #=#x, RECEPTION IP ADDRESS=b, PORT #=#y, TP=RTP, PT=#z)	\$26					
AUTHENTICATION & KEY EXCHANGE REQUEST (BY IP PACKET OR DATALINI (PROTOCOL TYPE=DTCP) FOR STREAM OF (TRANSMISSION IP ADDRESS=a, RECEPTION IP ADDRESS=b, PORT #=#y, TP=RTP, PT=#z)	( LAYER FRAME) PORT #=#x,					
AUTHENTICATION & KEY EXCHANGE PROCEDURE (BY IP PACKET OR DATALINK LAYER FRAME) (PROTOCOL TYPE=DTCP)	∽ S27					
S28 S29 ACQUI	RE DECRYPTION KEY					
FIG. 16						
TRANSMISSION DEVICE (IP ADDRESS=a)	RECEPTION DEVICE (IP ADDRESS=b)					
AUTHENTICATION & KEY EXCHANGE REQUEST (BY IP PACKET OR DATALINK L	AYER FRAME)					
AUTHENTICATION & KEY EXCHANGE PROCEDURE (BY IP PACKET OR DATALINK LAYER FRAME) (RANGE OF VALUE OF TARGE PAYLOAD TYPE=#z1-#z2)	S31 T DYNAMIC					
	S32					
S33 ~ ACQUII	RE DECRYPTION KEY					
AV CONTROL COMMAND (PLAY) (BY RTSP/TCP/IP), PT NEGOTIATION (PT=#z)						
ENCRYPT AV DATA ~ \$35	S34					
AV DATA (ENCRYPTED) (BY RTP/IP) (TRANSMISSION PORT #=#x, RECEPTION PORT #=#y, PT=#z)	S36					

### **FIG. 17**





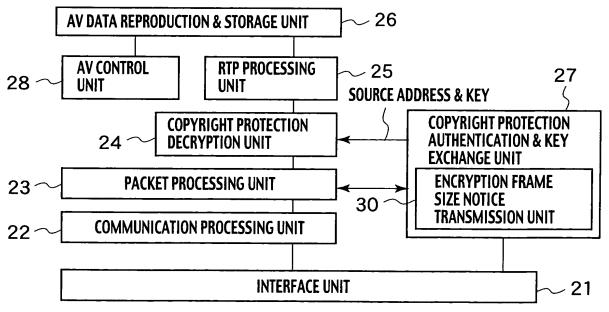
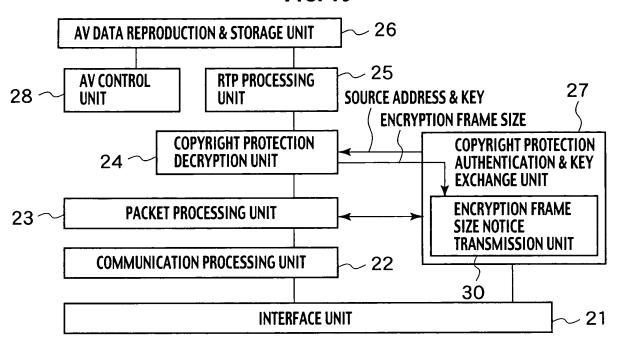
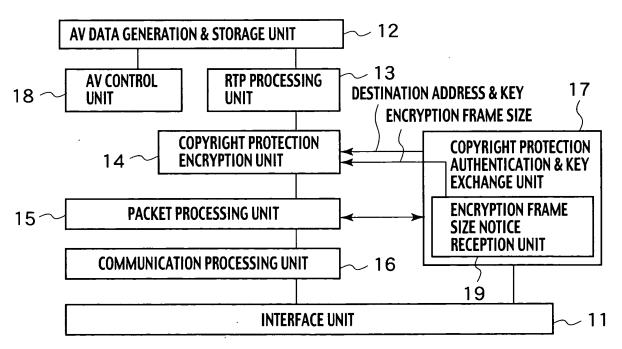


FIG. 19

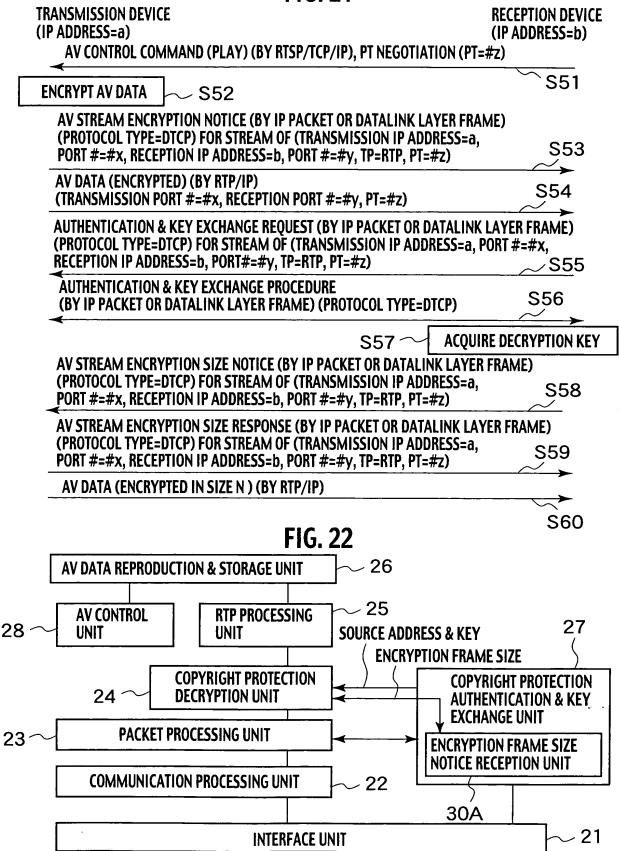


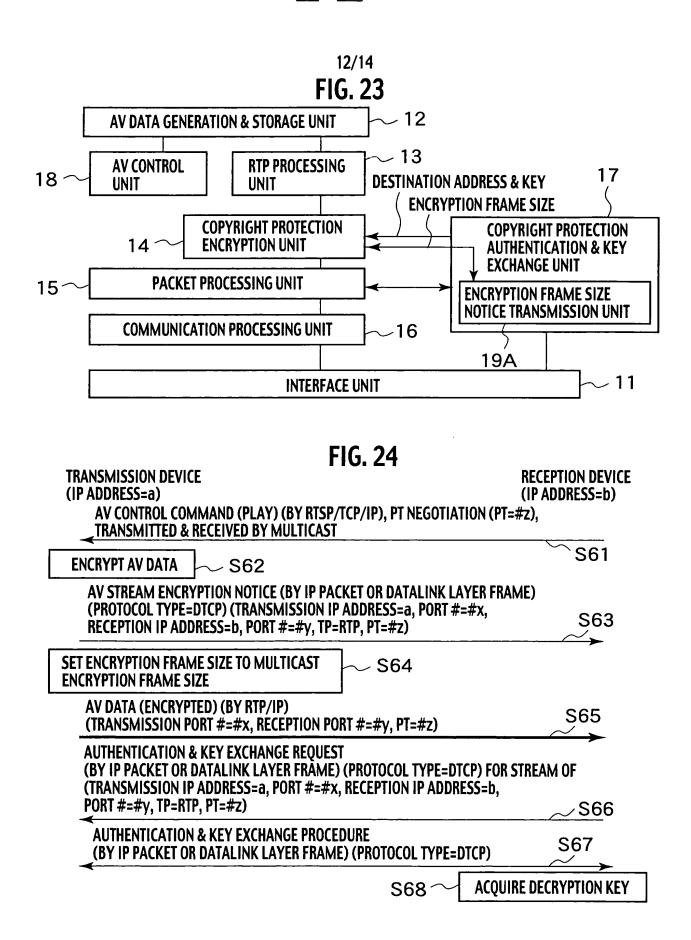
**FIG. 20** 



OBLON, SPIVAK, ET AL DOCKET #: 249170US2RD INV: Takeshi SAITO, et al. SHEET 11 OF 14

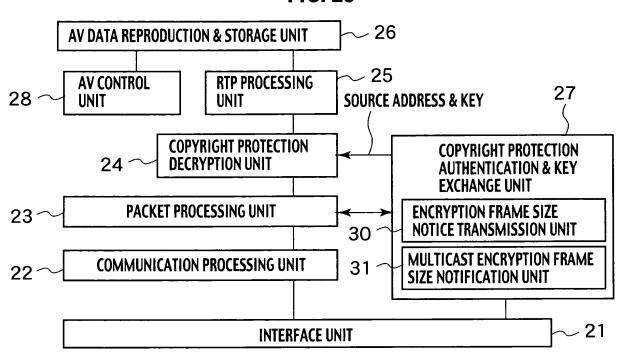
# 11/14 **FIG. 21**





13/14

## FIG. 25



# **FIG. 26**

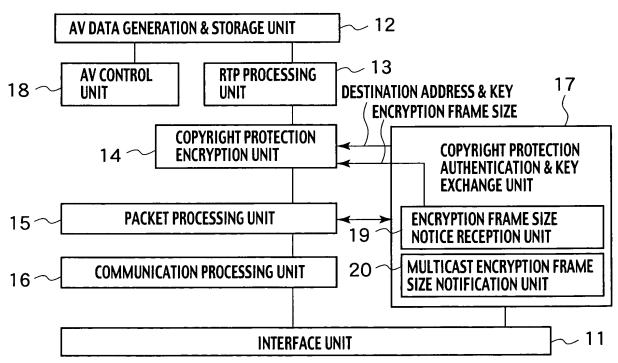


FIG. 27

## SIZE SPECIFICATION REQUEST PACKET

IP HEADER	TCP HEADER	COPYRIGHT PROTECTION COMMON CONTROL HEADER	ENCRYPTION FRAME SIZE REQUEST	SIZE VALUE
>	}	}	}	}
d21	d22	d23	d24	d25

FIG. 28

#### **SIZE SPECIFICATION RESPONSE PACKET**

IP HEADER	TCP HEADER	COPYRIGHT PROTECTION COMMON CONTROL HEADER	ENCRYPTION FRAME SIZE RESPONSE (PERMISSION / REJECTION)	SIZE VALUE (OPTION)
	}	}	· ·	
d31	d32	d33	d34	d35